ОРГАНИЗАЦИЯ РАБОТЫ С ПЕРСОНАЛОМ, ОБЛАДАЮЩИМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ, НА ПРИМЕРЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО КАЗЕННОГО УЧРЕЖДЕНИЯ «2-го ОТРЯДА ФЕДЕРАЛЬНОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ ПО ЧЕЛЯБИНСКОЙ ОБЛАСТИ»

Бобина Е.С.

ФГБОУ ВПО «Магнитогорский государственный технический университет имени Г.И. Носова», г. Магнитогорск, Россия

Издавна считалось, что тот, кто владеет информацией, владеет миром. Стремление сохранить втайне от других то, что дает преимущество и власть, является главной мотивацией людей в исторической перспективе. Многие в целях защиты своих интересов засекречивают информацию. Это приводит к постоянному совершенствованию средств и методов добывания охраняемой информации и к совершенствованию средств и методов защиты информации.

Рассекречивание закрытой информации какой-либо организации может привести как к небольшим финансовым потерям, так и к полному развалу организации. Следовательно, возникает острая необходимость защиты закрытой информации.

Стандарт ISO/IEC 17799 определяет информационную безопасность как обеспечение конфиденциальности, целостности и наличия информации.

Безопасность − это не только защита от преступных посягательств, но и обеспечение сохранности (особенно электронных) документов и информации, а также меры по защите важнейших документов и обеспечению непрерывности и/или восстановлению деятельности в случае катастроф.

Конфиденциальность − защита от несанкционированного доступа. Следующее определение конфиденциальности дает ФЗ «Об информации, информационных технологиях и о защите информации», в соответствии со ст. 2. п.7: конфиденциальность − обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Различают конфиденциальность внешнюю − как условие неразглашения информации во внешнюю среду, и внутреннюю − среди персонала. Конфиденциальность отражает ограничение, которое накладывает собственник информации на доступ к ней других лиц, т.е. собственник устанавливает правовой режим этой информации в соответствии с законом.

Конфиденциальная информация − документированная информация, т.е. зафиксированная на материальном носителе, доступ к которой ограничивается в соответствии с законодательством РФ. Содержание конфиденциальной информации документируется, зависит от компетенции и функций предприятия, учреждения или организации, характера их деятельности, взаимосвязей с другими субъектами. В свою очередь это содержание влияет на качество соответствующей области деятельности, организацию и надежность обработки и защиты документов.

Доступ к конфиденциальной информации − это получение разрешения руководителя на выдачу сотруднику (уполномоченному должностному лицу) конкретных сведений с учетом его служебных обязанностей.

По мнению большинства специалистов по безопасности информационных систем, главное внимание должно быть обращено на персонал, постоянно работающий с конфиденциальными документами и базами данных. Именно персонал является одним из главных распространителей конфиденциальности информации.

В решении проблемы информационной безопасности значительное место занимает выбор эффективных методов работы с персоналом, обладающим конфиденциальной информацией. Основными формами контроля качества работы персонала, повышения ими своих профессиональных знаний, в том числе в части защиты информации, можно назвать следующие:

- аттестация сотрудников;
- отчеты руководителей подразделений о работе подразделений и состоянии системы защиты информации;
- регулярные проверки руководителем фирмы и службой безопасности соблюдения сотрудниками требований системы защиты информации;
- самоконтроль сотрудников.

Можно отметить, что стабильность кадрового состава является важнейшей предпосылкой надежной информационной безопасности фирмы.

Рассмотрим работу учреждения ФГКУ «2 ОФПС по Челябинской области», его местонахождение, а также деятельность персонала данной организации.

Федеральная противопожарная служба осуществляет:

- оповещение населения об угрозе возникновения чрезвычайной ситуации, а также информирование о развитии чрезвычайной ситуации и действиях, предпринимаемых по ее ликвидации;
- принятие вызова по телефонным линиям о чрезвычайных ситуациях и информирование должностных лиц о выезде подразделений, обстановке на месте осуществляется диспетчером пожарной службы;
- оперативное управление другими видами пожарной охраны, силами и средствами, привлекаемыми для тушения пожаров на объектах, критически важных для страны;
- проводит противопожарную пропаганду и обучение населения мерам пожарной безопасности;
- организует и ведет официальный статистический учет и государственную статистическую отчетность по пожарам и их последствиям на территории Российской Федерации, показателям оперативной деятельности и ресурсам федеральной противопожарной службы.

Миссия предприятия − профилактика, оперативное тушение пожаров и аварийно-спасательные работы, отправка пожарных на защиту населения и территории от чрезвычайных ситуаций природного и техногенного характера.

Основной задачей деятельности службы – выполнение перечисленных основных целей, а также повышение качества устранения чрезвычайных ситуаций, внедрение инновационных технологий устранения ЧП.

Во главе предприятия стоит начальник отряда, который решает в основном управленческие вопросы и вопросы стратегического характера.

Начальник отдела кадров:

- руководит работниками отдела, а также структурными подразделениями, входящими в состав отдела кадров;
- возглавляет работу по комплектованию предприятия кадрами рабочих, служащих и специалистов требуемых профессий, специальностей и квалификации в соответствии с целями, стратегией и профилем предприятия;
- принимает участие в разработке кадровой политики и стратегии предприятия;
- осуществляет работу по подбору, отбору кадров на основе оценки их квалификации, личных и деловых качеств, контролирует правильность использования работников в подразделениях предприятия;
- организует учет личного состава, выдачу справок о настоящей и прошлой трудовой деятельности работников, хранение и заполнение трудовых книжек.

Начальник отдела кадров и работники этого отдела имеют дело с конфиденциальной информацией такой, как персональные данные сотрудников предприятия ФГКУ «2 ОФПС по Челябинской области». Из этого следует, что на отдел кадров ложатся обязанности защиты конфиденциальной информации предприятия.

В должностные обязанности бухгалтера входит:

- осуществление приема и контроля первичной документации бухгалтерского учета;
- отражение на счетах бухгалтерского учета операций, связанных с движением основных средств, денежных средств;
- выявление источников образования потерь и непроизводительных затрат;
- начисление заработной платы и премии сотрудникам противопожарной службы;
- формирование, хранение базы данных бухгалтерской информации, внесение изменения в справочную и нормативную информацию, используемую при обработке данных.

Начальник предприятия не в силах изменить внешнюю среду. Он должен изучать ее и приспосабливаться к ней. Он утверждает список должностных лиц, ответственных за принятие заявок, правильное и своевременное оформление этих заявок.

На основании анализа полученной информации можно сделать вывод, что в отделе кадров и архива находится конфиденциальная информация предприятия ФГКУ «2 ОФПС по Челябинской области».

Доступом лица к конфиденциальной информации является санкционированное ознакомление персонала должностным лицом предприятия и иных лиц с конфиденциальной информацией и ее носителями.

Разрешительная система доступа персонала предприятия предусматривает установление на предприятии единого порядка обращения с носителями сведений, составляющих коммерческую тайну, определение ограничений на доступ к ним различных категорий персонала (управленческого, административного и исполнительского уровней) и степени ответственности за сохранность указанных носителей сведений.

Основные условия доступа персонала к коммерческой информации включают:

- подписание работником обязательства о неразглашении сведений, составляющих коммерческую тайну, а также трудового договора;
- наличие у работника, оформленного в установленном порядке допуска к сведениям, составляющим коммерческую тайну;
- наличие утвержденных начальником предприятия должностных (функциональных) обязанностей сотрудника, определяющих круг его задачи объем необходимой для их решения информации;

Основная цель разрешительной системы доступа персонала к коммерческой тайне − исключение нанесения ущерба предприятию посредством несанкционированного распространения сведений, составляющих коммерческую тайну.

Под разглашением конфиденциальной информации понимаются умышленные или неосторожные действия, допущенные к персональным данным лиц, приведшие к преждевременному, не вызванному служебной необходимостью распространению указанной информации среди лиц, которым эта информация не была доведена в официально установленном порядке. Происходит утечка конфиденциальной информации − это несанкционированное распространение информации за пределы установленного физического пространства.

На предприятии ФГКУ «2 ОФПС по Челябинской области» к конфиденциальной информации относят персональные данные (далее ПДн) сотрудников, которые хранятся в отделе кадров. Персональные данные работника − это информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Персональные данные работника содержатся в основном документе персонального учета работников − личном деле работника.

Чтобы избежать несанкционированного доступа к персональным данным сотрудника противопожарной службы, личные дела не выдаются на руки работникам, на которых они заведены. Работник имеет право знакомиться только со своим личным делом в помещении кадровой службы под присмотром. Факт ознакомления с личным делом также фиксируется в описи дела.

Личные дела могут выдать во временное пользование, но при этом запрещается производить какие-либо исправления в сделанных записях, вносить новые записи, извлекать документы из личного дела, а также помещать в него новые. Разглашение конфиденциальных сведений, содержащихся в личном деле сотрудника службы, соответственно запрещается.

Изменения в личные дела вносятся только лицами, ответственными за их ведение − кадровиками. Тщательно проверяется сохранность документов при возврате личного дела, отсутствие повреждений, включения в дело других документов или подмены документов. Для хранения личных дел сотрудника используются запирающиеся металлические сейфы, шкафы, обеспечивающие полную сохранность документов и безопасность конфиденциальной информации.

Работник отдела кадров обязан правильно хранить, обрабатывать, передавать в архив документы предприятия и при необходимости осуществ-

лять выдачу социальных справок на основе документов по личному составу (ст. 62 Трудового кодекса Российской Федерации). Более того, в соответствии с Федеральным законом от 27.07.2006 N 152−ФЗ «О защите персональных данных» предприятия несут административную и уголовную ответственность за кражу, изменение, блокирование, копирование и разглашение персональных данных.

Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действуют требования по защите информации, вытекающие из нормативно-правовых документов предприятия.

При заключении трудового договора и оформлении приказа о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент включения данного лица в механизм обеспечения информационной безопасности.

Список использованных источников

1. *Алексенцев А.И. «Безопасность информационных технологий» 2000, № 3.*
2. *Веснин В.Р. «Управление персоналом. Теория и практика» М.: ТК «Велби», Проспект, 2008.*
3. *ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».*
4. *ГОСТ Р 53114-2008 «Защита информации. Обеспечение безопасности в организации».*
5. *Защита персональных данных [Электронный ресурс] − Режим доступа: URL: http://www.jetinfo.ru/stati/zaschita-personalnykh (дата обращения 18.01.2015).*
6. *Обработка, порядок хранения и передвижения персональных данных [Электронный ресурс] − Режим доступа: URL: http://hr-portal.ru/article/obrabotka-poryadok-hraneniya-i-peredvizheniya-personalnyh-dannyh (дата обращения 20.01.2015).*
7. *Организация работы с конфиденциальной информацией, составляющей коммерческую тайну [Электронный ресурс] − Режим доступа: URL: http://www.worklib.ru/laws/ml02/pages/10012477.php (дата обращения 23.01.2015).*
8. *Официальный сайт ФГКУ «2 ОФПС по Челябинской области» [Электронный ресурс] − Режим доступа: http://www.74.mchs.gov.ru/powers/detail.php?ID = 3275 (дата обращения 25.01.2015).*
9. *Персональные данные работника и их защита [Электронный ресурс] − Режим доступа: URL: http://hr-portal.ru/article/personalnye-dannye-rabotnika-i-ih-zashchita (дата обращения 25.01.2015).*
10. *Моделирование процесса формирования экономической грамотности студентов в структуре дополнительного образования вуза Сторожева Е.В., Валеев А.С., Кружилина Т.В., Сергеев А.Н. Сибирский педагогический журнал. 2011. № 12. С. 176-182.*
11. *Совершенствование качества внешнеэкономических связей предприятий в условиях интегрированного хозяйствования (на примере России и Казахстана) Елена Владимировна Сторожева монография / Е.В. Сторожева ; М-во образования и науки Российской Федерации, Федеральное агентство по образованию, ГОУ ВПО «Магнитогорский гос. ун-т». Магнитогорск, 2010.*